WILLIAM L. STERN (CA SBN 96105)
CLAUDIA M. VETÉSI (BAR NO. 233485)
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522
E-mail: wstern@mofo.com

Attorneys for Defendant and Counterclaimant
GAP INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JOEL RUIZ, On Behalf of Himself and All Others Similarly Situated, Plaintiff, v. GAP, INC., and DOES 1-9 inclusive, Defendants.	Case No. C 07-5739 SC **DEFENDANT GAP INC.'S REQUEST FOR JUDICIAL NOTICE IN SUPPORT OF MOTION FOR JUDGMENT ON THE PLEADINGS** Date: January 11, 2008 Time: 10:00 a.m. Room: Courtroom 1, 17th Floor Judge: Honorable Samuel Conti Complaint filed: November 13, 2007

Pursuant to Federal Rule of Evidence 201, Defendant GAP, Inc. ("GAP") hereby requests that this Court take judicial notice of the following:

1. *National Data Breach Analysis*, available at http://www.idanalytics.com/assets/pdf/National_DataBreach_FAQ.pdf, a true and correct copy of which is attached hereto as Exhibit A.

2. A list of California data breach incidents reported in the past two years, compiled from the website of the Privacy Rights Clearinghouse, available at http://privacyrights.org/ar/ChronDataBreaches.htm, a true and correct copy of which is attached hereto as Exhibit B.

This Court may take judicial notice, at any stage of the proceeding, of facts that are "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b); *Coremetrics, Inc. v. AtomicPark.com, LLC*, 370 F. Supp. 2d 1013, 1021 (N.D. Cal. 2005) (taking judicial notice of website). Accordingly, Defendant GAP requests that this Court take judicial notice of Exhibits A and B.

Dated: December 7, 2007

WILLIAM L. STERN
CLAUDIA M. VETÉSI
MORRISON & FOERSTER LLP

By /s/ William L. Stern
William L. Stern

Attorneys for Defendant and Counterclaimant
GAP INC.

EXHIBIT

A

FREQUENTLY ASKED QUESTIONS

WHAT DATA DID ID ANALYTICS STUDY?

ID Analytics studied the level of suspicious misuse of identity information experienced by the entire population of breach victims in ***four*** separate data breaches. The analysis covered approximately 500,000 consumer identities.

HOW IS THIS STUDY DIFFERENT FROM THE OTHER REPORTS THAT HAVE BEEN PUBLISHED?

This is the **ONLY** research available today that has looked at **ACTUAL** data breaches and examined how fraudsters are using them.

WHAT DID ID ANALYTICS DISCOVER?

ID Analytics discovered that:

- The calculated fraudulent misuse rate for consumer victims of the analyzed identity-level breach with the highest rate of misuse was 0.098 percent—less than one in 1,000 identities.
- Different breaches pose different degrees of identity fraud risk:
  - Intentional, identity-level breaches pose the greatest potential for harm to businesses and consumers due to fraudsters' sophisticated methods for profiting from identity information.
  - Account-level breaches do not appear to result in follow-on identity theft.
- In certain targeted data breaches, notices may have a deterrent effect. In one large-scale identity-level breach, thieves slowed their use of the data to commit identity theft after public notification.
- Criminals who stole the data in the breaches used identity data manipulation, or "tumbling" to avoid detection and to prolong the scam.
- Criminals are limited by practical considerations when using stolen IDs. This suggests that the smaller the intentional data breach, the higher the identity theft risk posed to the individual consumer impacted by a data breach.

  (As an example, it takes approximately five minutes to fill out a credit application. At this rate, it would take a fraudster working full-time – averaging 6.5 hours a day, five days a week, 50 weeks a year -- over 50 years to fully utilize a breached file consisting of one million consumer identities. If the criminal outsourced the work at a rate of $10 an hour in an effort to use a breached file of the same size in one year, it would cost that criminal about $830,000.)

CAN THE BREACHES STUDIED BE DESCRIBED MORE FULLY?

Two of the breaches were ***identity-level*** breaches. An identity-level breach involves the most sensitive data available – names, Social Security numbers (SSNs), dates of birth, addresses, and other personally-identifiable information. One breach was a targeted breach. In other words, the breach occurred not because data was lost, but because thieves actually intended to steal the personal information. The other breach was not a targeted breach.

Two of the breaches were ***account-level*** breaches: An account-level breach involves the name and credit card numbers.

HOW MUCH IDENTITY THEFT DID ID ANALYTICS FIND IN THE ACCOUNT-LEVEL BREACHES?

There was no evidence that the breached file was being exploited by fraudsters to perpetrate large-scale identity fraud scams. ID Analytics did not study the rate of misuse of the actual credit card information.

HOW MUCH IDENTITY THEFT DID ID ANALYTICS FIND IN THE IDENTITY-LEVEL BREACHES?

The calculated fraudulent misuse rate for consumer victims of the analyzed identity-level breach with the highest rate of misuse was 0.098 percent—less than one in 1,000 identities.

CAN ID ANALYTICS OFFER SOME EXPLANATION WHY THE MISUSE FROM DATA BREACHES IS LOWER THAN EXPECTED?

While initially surprising, the seemingly low misuse rate recognizes a fundamental truth about identity fraud. It is the fraud ring's available resources that determine how much attempted misuse follows a targeted, identity-level data breach. Fraud rings simply do not have the time or manpower to use hundreds of thousands of identities available to them in their nefarious pursuits.

Think about this practically. If a fraudster spent five minutes to fill out a new account application that is likely to be approved, one application per unique identity, worked 6.5 hours per day, it would take that individual over 50 years to utilize a breached file of one million consumer identities. This scenario overlooks other practicalities, such as procuring the applications and the need to launder the proceeds over time.

The misuse rate could increase drastically if the current black market for "identities" remains unimpeded and becomes more centralized and efficient.

ISN'T IT POSSIBLE THAT THIEVES ARE WAREHOUSING THE DATA AND COULD USE IT TO COMMIT FRAUD IN THE FUTURE?

Yes, that is possible. Once thieves have used a breach file for a crime, continued identity monitoring is necessary.

ID Analytics found evidence of data warehousing in the identity-level breach. Over the 24-month observation window for the identity data breach, there was a 12-month pattern of low rates of misuse. The thieves actually mimicked consumer behavior so it would be harder for credit card companies to detect them. Use spiked after the breach was discovered.

HAS ID ANALYTICS STUDIED ENOUGH BREACHES TO MAKE ANY MEANINGFUL CONCLUSIONS?

ID Analytics believes more research needs to be done. But this is the **ONLY** research available today that has looked at **ACTUAL** breaches and examined how fraudsters are using them.

The identity-level breach that was studied was a particularly nefarious and coordinated attack on personal data.

WAS THIS A SURVEY?

No. Using its ID Network, ID Analytics examined every single identity that was compromised in each breached file. In other words, this study looked at how data breaches affected hundreds of thousands of identities in the months after those breaches.

CAN YOU TELL US WHICH BREACHES THESE WERE?

In order to preserve confidentiality and to comply with legal non-disclosure obligations, ID Analytics can not identify the names of the entities whose data was compromised.

For more information, please email *marketinginfo@idanalytics.com* or visit *www.idanalytics.com*

EXHIBIT
B

Exhibit B

California Data Breach Incidents Reported in the Past Two Years[1]

Date	Entity	Description
Jan. 18, 2005	Univ. of CA, San Diego	Hacker breached the security of two University computers that stored the Social Security numbers ("SSNs") and names of students and alumni of UCSD Extension.
Feb. 12, 2005	Science Applications International Corp.	Thieves broke into a SAIC facility and stole computers containing names, SSNs, and other personal information of past and current employees.
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop.
March 11, 2005	Kaiser Permanente	Disgruntled employee posted information on her blog noting that Kaiser Permanente included private patient information on systems diagrams posted on the Web.
March 22, 2005	Calif. State Univ., Chico	Hacking.
March 23, 2005	Univ. of CA., San Francisco	Hacking.
April 5, 2005	Univ. of CA, Davis	Names and SSNs of students, faculty, visiting speakers and staff may have been compromised when a hacker accessed a main computer.
April 6, 2005	University of CA, San Francisco	Server in the accounting and personnel departments was hacked. It contained information on 7,000 students, faculty, and staff members. The affected individuals were notified March 23.
April 8, 2005	San Jose Med. Group	Stolen computer.
April 14, 2005	Calif. Fastrack	Dishonest Insider.
April 15, 2005	CA Dept. of Health Service	Stolen laptop.

[1] This list was complied on November 28, 2007 from the website of the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization. This Exhibit consists of all data breaches listed on that website for the State of California. That website can be found at http://www.privacyrights.org/ar/ChronDataBreaches.htm.

Date	Entity	Description
May 11, 2005	Stanford Univ.	Hacking.
July 1, 2005	Univ. of CA, San Diego	Hacking.
July 19, 2005	Univ. of Southern Calif.	Hacking.
July 30, 2005	San Diego Co. Employees Retirement Assoc.	Hacking.
July 30, 2005	Calif. State Univ., Dominguez Hills	Hacking.
July 31, 2005	Cal Poly-Pomona	Hacking.
Aug. 9, 2005	Sonoma State Univ.	Hacking.
Aug. 17, 2005	Calif. State University, Stanislaus	Hacking.
Aug. 30, 2005	Calif. State University, Chancellor's Office	Hacking.
Sept. 19, 2005	Children's Health Council	Stolen backup tape.
Nov. 4, 2005	Keck School of Medicine, USC	Stolen computer.
Dec. 1, 2005	Univ. of San Diego	Hacking. Faculty, students and employee tax forms containing SSNs.
Jan. 17, 2006	City of San Diego, Water & Sewer Dept.	Dishonest employee accessed customer account files, including SSNs, and committed identity theft on some individuals.
Jan. 21, 2006	California Army National Guard	Stolen briefcase with personal information of National Guardsmen including a "seniority roster," SSNs and dates of birth.
Feb. 17, 2006	Calif. Dept. of Corrections, Pelican Bay	Inmates gained access to files containing employees' Social Security numbers, birth dates and pension account information stored in warehouse.

Date	Entity	Description
Mar. 2, 2006	Los Angeles Cty. Dept. of Social Services	File boxes containing names, dependents, SSNs, telephone numbers, medical information, employer, W-2, and date of birth were left unattended and unshredded.
Mar. 11, 2006	CA Dept. of Consumer Affairs	Mail theft. Applications of DCA licensees or prospective licensees for CA state boards and commissions were stolen. The forms include full or partial SSNs, driver's license numbers, and potentially payment checks.
Mar. 16, 2006	Bananas.com	Hacker accessed names, addresses, phone numbers and credit card numbers of customers.
Mar. 24, 2006	CA State Employment Development Division	Computer glitch sends state Employment Development Division 1099 tax forms containing SSNs and income information to the wrong addresses, potentially exposing those taxpayers to identity theft.
Mar. 30, 2006	Marines	Portable drive lost that contains personal information used for research on re-enlistment bonuses.
May 5, 2006	Wells Fargo	Computer containing names, addresses, SSNs and mortgage loan deposit numbers of existing and prospective customers may have been stolen while being delivered from one bank facility to another.
June 17, 2006	CA Dept of Health Services	CDHS documents were inappropriately emptied from an employee's cubicle on June 5 and 9 rather than shredded. The documents contained state employees and other individuals applying for employment with the state including names, addresses, SSNs and home and work telephone numbers. They were mostly expired state employment certification lists, but also included requests for personnel action, copies of e-mail messages and handwritten notes.
June 23, 2006	San Francisco State Univ.	A faculty member's laptop was stolen from a car on June 1 that contained personal information of former and current students including SSNs, and names and in some instances, phone numbers and grade point averages.
June 23, 2006	CA Dept of Health Services	A box of Medi-Cal forms from December 2005 were found in the cubicle of a CDHS employee. The claim forms contained the names, addresses, SSNs and prescriptions for beneficiaries or their family members.
June 28, 2006	AAAAA Rent-A-Space	Customer's account information including name, address, credit card, and SSN was easily accessible due to a security gap in its online payment system.

Date	**Entity**	**Description**
July 14, 2006	California Polytechnic State University	Laptop computer was stolen from the home of a physics department professor July 3. It included names and SSNs of physics and astronomy students from 1994-2004.
July 27, 2006	Kaiser Permanente Northern Calif. Office	Laptop was stolen containing names, phone numbers, and the Kaiser number for each HMO member. The data file did not include SSNs. The data was being used to market Hearing Aid Services to Health Plan members.
July 27, 2006	Los Angeles County	Laptop was stolen from the home of a community and senior services employee. It contained information on LA County employees.
July 27, 2006	Los Angeles Co., Community Development Commission	Computer hacker located in Germany gained access to the CDC's computer system, containing personal information on 4,800 public housing residents.
July 27, 2006	Los Angeles County, Adult Protective Services	11 laptops were stolen from the Burbank office. It is not clear what type of personal information was included.
July 28, 2006	Riverside, Calif., city employees	The SSNs and financial information regarding 401(k) accounts was accidentally e-mailed to 2,300 city employees due to a computer operator's error. The data was intended for the city payroll dept.
Aug. ?, 2006	CoreLogic for ComUnity Lending	Computer with customers' data was stolen from its office. Data includes names, SSNs, and property addresses related to an existing or anticipated mortgage loan.
Aug. 1, 2006	Dollar Tree	Customers of the discount store have reported money stolen from their bank accounts due to unauthorized ATM withdrawals. Data may have been intercepted by a thief's use of a wireless laptop computer with the thief then creating counterfeit ATM cards and using them to withdraw money.
Aug. 16, 2006	Chevron	Laptop was stolen from "an employee of an independent public accounting firm" who was auditing its benefits plans. The theft apparently occurred Aug. 5. Files contained SSNs and sensitive information related to health and disability plans.
Aug. 17, 2006	Williams-Sonoma	Laptop was stolen from the Los Angeles home of a Deloitte & Touche employee who was conducting an audit for W-S. Computer contained employees' payroll information and SSNs.

Date	Entity	Description
Aug. 18, 2006	Calif. Dept. of Mental Health	Computer tape with employees' names, addresses, and SSNs has been reported missing. Employees were notified Aug. 17 by e-mail.
Aug. 29, 2006	AT&T via vendor that operates an order processing computer	Computer hackers accessed credit card account data and other personal information of customers who purchased DSL equipment from AT&T's online store. The company is notifying "fewer than 19,000" customers.
Sept. 1, 2006	Wells Fargo via unnamed auditor	Laptop and data disk were stolen from the locked trunk of an unnamed auditor, hired to audit the employees' health plan. Data included names, SSNs, and information about drug claim cost and dates from 2005, but no prescription information said the company.
Sept. 8, 2006	Linden Lab	Hacker accessed its Second Life database through web servers. The affected data included unencrypted account names, real life names, and contact information, plus encrypted account passwords and payment information. Second Life is a 3-D virtual world.
Sept. 15, 2006	Mercy Medical Center	A memory stick containing patient information was found July 18 by a local citizen on the ground at the County Fairgrounds near the hospital's information booth. It was returned to the hospital 4 weeks later. Data included names, SSNs, birthdates, and medical records.
Sept. 18, 2006	Howard, Rice, Nemerovski, Canady, Falk & Rabkin law firm via its auditor Morris, Davis & Chan	Laptop was stolen from the trunk of the car of the law firm's auditor, containing confidential employee pension plan information -- names, SSNs, remaining balances, 401(k) and profit-sharing information.
Oct. 5, 2006	San Juan Capistrano Unified School District	Five computers stolen from the HQ of San Juan Capistrano Unified School District likely contain the names, SSNs and dates of birth of district employees enrolled in an insurance program.
Oct. 6, 2006	Camp Pendleton Marine Corps base via Lincoln B.P. Management	Laptop missing from Lincoln B.P. Management Inc. holds personally identifiable data about 2,400 Camp Pendleton residents.

Date	Entity	Description
Oct. 17, 2006	City of Visalia, Recreation Division	Personally identifiable information of approximately 200 current and former Visalia Recreation Department employees was exposed when copies of city documents were found scattered on a city street.
Oct. 27, 2006	Gymboree	A thief stole 3 laptop computers from Gymboree's corporate headquarters. They contained unencrypted human resources data (names and SSNs) of thousands of workers.
Nov. 9, 2006	Four ARCO gas stations	Thieves used card skimmers to steal bank account numbers and PIN codes from gas station customers and used the information to fabricate debit cards and make ATM withdrawals.
Nov. 28, 2006	Cal State Los Angeles, Charter College of Education	An employee's USB drive was inside a purse stolen from a car trunk. It contained personal information on 48 faculty members and more than 2,500 students and applicants of a teacher credentialing program. Information included names, SSNs, campus ID numbers, phone numbers, and e-mail addresses.
Dec. 12, 2006	University of California - Los Angeles	Hacker(s) gained access to a UCLA database containing personal information on current and former students, current and former faculty and staff, parents of financial aid applicants, and student applicants, including those who did not attend. Exposed records contained names, SSNs, birth dates, home addresses, and contact information. About 3,200 of those notified are current or former staff and faculty of UC Merced and current and former staff of UC's Oakland headquarters.
Dec. 21, 2006	Santa Clara County employment agency	Computer stolen from the agency holds the SSNs of approximately 2,500 individuals.
Jan. 4, 2007	Unnamed medical center, via Newark Recycling Center	An individual found unshredded medical records in 36 boxes at the Newark Recycling Center.
Jan. 17, 2007	Rincon del Diablo Municipal Water District	2 computers were stolen from the district office. One included names and credit card numbers of customers.

Date	**Entity**	**Description**
Jan. 26, 2007	Vanguard University	2 computers were discovered stolen from the financial aid office. Data included names, SSNs, dates of birth, phone numbers, driver's license numbers, and lists of assets.
Feb. 2, 2007	Indian Consulate via Haight Ashbury Neighborhood Council recycling center	Visa applications and other sensitive documents were accessible for more than a month in an open yard of a recycling center. Information included applicants' names, addresses, phone numbers, birthdates, professions, employers, passport numbers, and photos. A sampling of documents indicated that the paperwork included everyone who applied in the Western states from 2002-2005. Applicants were current and former executives of major Bay Area companies that have operations in India.
Feb. 14, 2007	Kaiser Medical Center	A doctor's laptop was stolen from the Medical Center containing medical information of 22,000 patients. But only 500 records contained SSNs.
Feb. 15, 2007	City College of San Francisco	Names, grades, and SSNs were posted on an unprotected Web site after summer session in 1999. CCSF stopped using SSNs as studens IDs in 2002.
Mar. 2, 2007	Calif. Dept. of Health Services	Benefit notification letters containing names addresses, Medicare Part D plan names and premium payment amounts of some individuals enrolled in the California AIDS Drug Assistance Program (ADAP) were mailed to another enrollee.
Mar. 7, 2007	Los Rios Community College	Student information including SSNs were accessible on the Internet after the school used actual data to test a new onine application process in October.
Mar. 9, 2007	California National Guard	A computer hard drive containing SSNs, home addresses, birth dates and other identifying information of California National Guard troops deployed to the U.S.-Mexico border was stolen.
Mar. 20, 2007	Tax Service Plus	Thieves stole the company's backup computer, which contained financial data on thousands of tax returns dating back three years.
Mar. 30 2007	Los Angeles County Child Support Services	Three laptops containing personal information including about 130,500 SSNs — most without names, 12,000 individuals' names and addresses, and more than 101,000 child support case numbers were apparently stolen from the department's office.

Date	Entity	Description
Mar. 30, 2007	Naval Station San Diego's Navy College Office	Three laptops were reported missing that may contain Sailors' names, rates and ratings, SSNs, and college course information. The compromise could impact Sailors and former Sailors homeported on San Diego ships from January 2003 to October 2005 and who were enrolled in the Navy College Program for Afloat College Education.
Apr. 4, 2007	UC San Francisco	An unauthorized party may have accesed the personal information including names, SSNs, and bank account numbers of students, faculty, and staff associated with UCSF or UCSF Medical Center over the past two years by compromising the security of a campus server.
Apr. 18, 2007	Univ. of CA, San Francisco	A computer file server containing names, contact information, and SSNs for study subjects and potential study subjects related to studies on causes and cures for different types of cancer was stolen from a locked UCSF office. For some individuals, the files also included personal health information.
Apr. 21, 2007	Albertsons	Credit and debit card numbers were stolen using bogus checkout-line card readers resulting in card numbers processed at those terminals being captured and some to be misused.
Apr. 27, 2007	Google Ads	Top sponsored Google ads linked to 20 popular search terms were found to install a malware program on users' computers to capture personal information and used to access online accounts for 100 different bank.
May 11, 2007	Univ. Calif. Irvine Medical Center	About 1,600 file boxes stored in an off-site university warehouse were discovered missing. Some of the files included patients' names, addresses, SSNs and medical record numbers.
May 15, 2007	San Diego Unified School District	In a letter to its employees, the School District said it had been notified by law enforcement that a former employee had access to personal identification information of "a select number of district employees." Those employees were notified separately. The letter said it has "no specific knowledge of any attempted fraud..."
May 31, 2007	Priority One Credit Union	Priority One Credit Union sent out election ballots to members with SSNs and account numbers printed on the outside of the envelopes

Date	Entity	Description
June 1, 2007	Fresno County/Refined Technologies Inc.	Missing computer disk contains names, addresses, SSNs numbers. The county sent it by courier to a software vendor's office in San Jose to determine workers' eligibility for health care benefits. The software company, Refined Technologies Inc., said they never received the disk.
June 14, 2007	Hamburger Hamlet Restaurant	Former waitress made off with the credit or debit card numbers of at least half a dozen patrons - and possibly as many as 40. Already, about $16,300 in unauthorized charges have been linked to the scam.
June 25, 2007	Fresno County	A disk containing information pertaining to home health-care workers -- including their names, addresses and SSNs was lost.
June 27, 2007	University of California, Davis	Computer-security safeguards were breached and accessed information including the applicants' names, birth dates and, in most cases, SSNs.
July 13, 2007	City of Encinitas	Credit card or checking account information and addresses of people who had enrolled in Encinitas' youth recreation programs was inadvertently posted on the city's Web site.
July 17, 2007	Kingston Technology Co.	Security breach that remained undetected until "recently" may have compromised the names, addresses and Credit Card details of online customers.
July 20, 2007	Science Applications International Corp.	Pentagon contractor may have compromised personal information. Information such as names, addresses, birth dates, SSNs and health information about military personnel and their relatives because it did not encrypt data transmitted online.
July 28, 2007	Yuba County Health and Human Services	A laptop stolen from a building contained personally identifiable information of individuals whose cases were opened before May 2001. The laptop was being used as a backup system for the county's computer system. The data include SSNs, birth dates, driver's license numbers and other private information.
Aug. 6, 2007	Verisign	A laptop containing extensive personal information on an undisclosed number of VeriSign employees was stolen from an employee's car. The information included names, addresses, Social Security numbers, dates of birth, telephone numbers, and salary records.

Date	**Entity**	**Description**
Aug. 22, 2007	California Public Employees' Retirement System	Roughly 445,000 retirees across the state received the brochures announcing an upcoming election to fill a rare vacancy on the board of the California Public Employees' Retirement System. All or a portion of each person's SSN appeared without hyphens on the address panel.
Sept. 9, 2007	De Anza College	Thousands of former students might be at risk for identity fraud after an instructor's laptop computer, containing students' personal information, was stolen last month. The computer contained the students' names, addresses, grades and in many cases SSNs.
Sept. 9, 2007	McKesson	McKesson Health-care services company, is alerting thousands of its patients that their personal information is at risk after two of its computers were stolen from an office.
Oct. 8, 2007	Semtech	Laptop computer and other personal belongings were stolen from one of Semtech's vendors. The computer was not stolen from a Semtech facility, but may have contained computerized data relating to Semtech employees. Semtech declined to provide further details of the incident, such as what personal employee data may have been put at risk, when the theft happened or how long it took the company to inform its workers of the potential breach.
Nov. 6, 2007	Butte Community Bank	A laptop with customers' personal information including names, addresses, SSNs and bank account numbers was stolen from Butte Community Bank.